UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,975	02/04/2002	Michael J. Wookey	P7235	4232

32658 7590 02/15/2007

HOGAN & HARTSON LLP
ONE TABOR CENTER, SUITE 1500
1200 SEVENTEEN ST.
DENVER, CO 80202

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,975	WOOKEY ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/21/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 is pending.

2. This is a final rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 10-11, and 13-16 are rejected under 35 U.S.C. 102(e) as being anticipated by, ET Britt, Jr. et al. (US 6,230,319).

As per claim 1:

Britt, Jr. et al. discloses a method of automatically reconfiguring a component of a remote services network system comprising the steps of:

detecting a communication error related to a component of said network; **[col.8, lines 15-16]**

identifying a configuration parameter associated with the occurrence of said communication error; **[col.8, lines 26-30]**

obtaining corrected configuration data relating to said configuration parameter; and **[col.8, lines 32-33]**

automatically installing said corrected configuration data on said component to restore communication with said remote services network. **[col.8, lines 35-39 and col.12, lines 25-35; The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration data or configuration data that has been detected and identified as inconsistent state or error data that has been communicated in the network (col.8, lines 15-16). Specification states data configuration parameters are stored on servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). Britt, Jr. discloses data includes various configuration parameters, which can also refer as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-53). Hence, Britt reads on the claimed configuration parameter. Further, Britt discloses the system detects an error condition by verifying which is a process of identifying if the contents in the flash memory are valid or invalid (col.8, lines 10-11). Britt teaches the identified invalid contents are the corrupt information that needs to be replaced with correct information (col.8, lines 28-35). Thus, the corrupt information that has been detected and identified as error condition reads on the claimed configuration parameter associated with the occurrence of communication error.]**

As per claim 2: **See col.8, lines 26-30;** discussing communication error comprising

an error in the identity of said component.

As per claim 3: **See col.11, lines 41-44 and col.12, lines 25-35;** discussing communication error comprising an error related to connectivity of said component to said remote services network.

As per claim 10:

Britt discloses a remote services system, comprising:

a system component in communication with said remote services system, **[col.4, lines 32-41 and col.6, lines 58-61]** said component having a plurality of stored data parameters for maintaining communication with said remote services system; **[col.7, lines 51-55]**

a data base containing valid configuration data parameters for maintaining communication of said system component with said remote services system; and **[col.7, lines 31-36]**

a communication module operable to detect a communication error between said system component and said remote services system **[col.11, lines 41-44]** and to correct said communication error **[col.8, lines 15-16 and 26-30]** by obtaining valid configuration data parameters from said data base **[col.8, lines 32-33]** and installing said valid configuration data parameters on said system component. **[col.8, lines 35-39 and col.12, lines 25-35; The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration data or configuration data that has been detected and identified as inconsistent state or**

error data that has been communicated in the network (col.8, lines 15-16). Specification states data configuration parameters are stored on servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). Britt, Jr. discloses data includes various configuration parameters, which can also refer as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-53). Hence, Britt reads on the claimed configuration parameter. Further, Britt discloses the system detects an error condition by verifying which is a process of identifying if the content in the flash memory is valid or invalid (col.8, lines 10-11). Britt teaches the identified invalid contents are the corrupt information that needs to be replaced with correct information (col.8, lines 28-35). Thus, the corrupt information that has been detected and identified as error condition reads on the claimed configuration parameter associated with the occurrence of communication error.]

As per claim 11: **See col.8, lines 26-30;** discussing communication error comprises an error in the identity of said component.

As per claim 13: **See col.8, lines 15-16 and 26-30 and col.11, lines 41-44;** discussing communication error comprises an error related to connectivity of said component to said remote services network.

As per claim 14: **See col.7, lines 31-36 and col.9, lines 9-21;** discussing an application server, said application server being operable to obtain valid configuration data parameters from said data base and to transmit said valid configuration data parameters to said system component in response to an instruction received from said

communication module.

As per claim 15: **See col.7, lines 31-36;** discussing database residing on a server controlled by a service provider.

As per claim 16: **See col.10, lines 51-61;** discussing a internet web site for providing limited access to said data base residing on said server controlled by said service provider.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 4-9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Britt, Jr. et al. (US 6,230,319), and further in view of Howard, Jr. et al. (US 6,442,690).

As per claim 4:

The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration data or configuration data that has been detected and identified as inconsistent state or error data that has been communicated in the network (col.8, lines 15-16). Specification states data configuration parameters are stored on

servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). Britt, Jr. discloses data includes various configuration parameters, which can also refer as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-53). Hence, Britt reads on the claimed configuration parameter. Further, Britt discloses the system detects an error condition by verifying which is a process of identifying if the contents in the flash memory are valid or invalid (col.8, lines 10-11). Britt teaches the identified invalid contents are the corrupt information that needs to be replaced with correct information (col.8, lines 28-35). Thus, the corrupt information that has been detected and identified as error condition reads on the claimed configuration parameter associated with the occurrence of communication error. However, Britt, Jr. fails to include a client certificate.

Howard, Jr. et al. disclose an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS

desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the certificate has been used and the identity of the device (col.10, lines 6-15 and col.23, lines 61-67). Howard discloses the certificate is provided the IKMS over the public network where the certificate is validated verifies the device ID, and the certificate is associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

As per claim 5:

The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration data or configuration data that has been detected and identified as inconsistent state or error data that has been communicated in the network (col.8, lines 15-16). Specification states data configuration parameters are stored on servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). Britt, Jr. discloses data includes various configuration parameters, which can also refer as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-53). Hence, Britt reads on the claimed configuration parameter. Further, Britt discloses the system detects an error condition

by verifying which is a process of identifying if the contents in the flash memory are valid or invalid (col.8, lines 10-11). Britt teaches the identified invalid contents are the corrupt information that needs to be replaced with correct information (col.8, lines 28-35). Thus, the corrupt information that has been detected and identified as error condition reads on the claimed configuration parameter associated with the occurrence of communication error. However, Britt, Jr. fails to include a client certificate.

Howard, Jr. et al. disclose an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the certificate has been used and the identity of the device (col.10, lines 6-15 and col.23, lines 61-67). Howard discloses the certificate is provided the IKMS over the public

network where the certificate is validated verifies the device ID, and the certificate is associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

As per claim 6: **as rejected in claim 4.**

As per claim 7: **See Britt, Jr. on col.12, lines 25-35;** discussing the step of revalidating communications of said component with said remote services system.

As per claim 8: **as rejected in claim 5.**

As per claim 9: **See Britt, Jr. on col.12, lines 25-35;** discussing the step of revalidating communications of said component with said remote services system.

As per claim 12:

The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration data or configuration data that has been detected and identified as inconsistent state or error data that has been communicated in the network (col.8, lines 15-16). Specification states data configuration parameters are stored on servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). Britt, Jr. discloses data includes various configuration parameters, which can also refer as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-53). Hence, Britt reads on the claimed

configuration parameter. Further, Britt discloses the system detects an error condition by verifying which is a process of identifying if the contents in the flash memory are valid or invalid (col.8, lines 10-11). Britt teaches the identified invalid contents are the corrupt information that needs to be replaced with correct information (col.8, lines 28-35). Thus, the corrupt information that has been detected and identified as error condition reads on the claimed configuration parameter associated with the occurrence of communication error. However, Britt, Jr. fails to include a client certificate.

Howard, Jr. et al. disclose an integrated key management system that can support key generation and key distribution for numerous types of equipment (col.6, lines 1-2). Howard discloses IKMS can provide secure storage of key material and can allow for key recovery during disasters, equipment failure, etc., where it can support secure automated distribution of keys to equipment and rapid redistribution of previously distributed key material to restore secure communications services (col.6, lines 14-20). Howard discusses the View Key Inventory function that allows an operator to list all key material held securely in the IKMS database (col.19, lines 6-9) and the View Network Connectivity function lists the communication relationship defined within IKMS and show the type of cryptographic protection provided by this communication relationship (col.19, lines 19-23). There also includes a CPE error indicator at the bottom of the IKMS desktop where this can show communications error (col.16, lines 13-19 and col.19, lines 54-56). Howard discloses IKMS communicates with the device over open networks and exchanges certificate information where verification ensures that this is the first time the certificate has been used and the identity of the device (col.10, lines 6-15 and col.23,

lines 61-67). Howard discloses the certificate is provided the IKMS over the public network where the certificate is validated verifies the device ID, and the certificate is associated (col.26, lines 13-32). Therefore, it would have been obvious for a person of ordinary skills in the art to include a certificate as taught by Howard, Jr. with the teaching of automatically reconfiguring a component of a remote services network system as taught by Britt, Jr. because the certificate authenticates and verifies the device and its communications.

Response to Arguments

5. Applicant's arguments filed 11/21/2006 have been fully considered but they are not persuasive.

The argument on page 2 that Britt fails to identify a configuration parameter associated with an identified communication error is traversed because claimed invention does not have the limitation of an identified communication error. Claim 1 broadly recites identifying a configuration parameter associated with the occurrence of said communication error. As for the prior art, Britt teaches the processing system includes memory means for storing the information, detection means for detecting an interruption in the downloading process, and sustaining means for sustaining operation of the process system (col.3, lines 1-4). Britt discloses the system detects an error condition and verifies if the contents in the flash memory are valid or invalid (col.8, lines

10-16). Britt also shows an example if the contents are not valid which are corrupted or otherwise found to represent an inconsistent state (col.8, lines 28-30). To identify something (i.e. error condition or communication error), it is necessary to be able to establish or determine (i.e. the error or what may have caused an out of the ordinary condition) if something have been detected. Britt discloses detecting an interruption or an error condition such that corrupted information is found (col.8, lines 28-30) involves identifying the corrupt information or content associated with an error condition (col.8, lines 32 and 36). Thus, Britt reads on the claimed identifying a configuration parameter associated with the occurrence of said communication error.

The argument on page 3:

Examiner traverses the argument where Britt lacks teaching or suggestion of the identification of a configuration parameter associated with the occurrence of the communication error. Claim 1 recites identifying a configuration parameter associated with the occurrence of said communication error. Please see above with regard the claimed identifying a configuration parameter associated with the occurrence of said communication error.

Examiner also traverses the argument that Britt is silent on obtaining corrected configuration data relating to the configuration parameter that is associated with the occurrence of the communication error. As acknowledged by applicant that Britt discloses data being downloaded could comprise connection scripts used to establish network communication, then Examiner also points out that Britt discusses data includes various configuration parameters (i.e. images, sounds, connection scripts used

to establish communication with the server, etc.) (col.7, lines 51-55). Thus, the data that includes configuration parameter relates to communication information, instructions, or content. These data items can be overridden by storing alternate data items in the flash memory where the validity of all contents of the flash memory is verified (col.7, lines 55-63 and col.8, lines 24-30). Therefore, Britt discloses data or content that includes various configuration parameters as the claimed configuration parameters that are verified and if invalid is the corrupt information associated with data that includes various configuration parameters (col.8, lines 32 and 36). Therefore, Britt reads on the claimed obtaining corrected configuration data relating to the configuration parameter that is associated with the occurrence of the communication error.

It is also traversed that Britt fails to disclose automatically installing the corrected configuration data to restore communications with the network. Britt discloses obtaining corrected configuration data relating to the configuration parameter is where the corrupt information (as established earlier) is replaced by correct information (col.8, lines 33-34). Britt teaches the processing system includes detection means for detecting an interruption in the downloading process and sustaining means for sustaining operation of the process system (col.3, lines 1-4). Britt allows errors in the programming or data to be detected and automatically corrected by performing the error download routine with out intervention by the user (col.8, lines 35-39). Thus, Britt reads on the claimed automatically installing the corrected configuration data to restore communications with the network.

The argument on page 4:

Examiner traverses the argument regarding the term occurrence where applicant directs to the specification (pg.27), the parameter associated with the occurrence of the communication error is properly interpreted as the cause of the communication error and that a corrupt file that is a result of a communication error as disclosed in Britt is not associated with the error's occurrence as properly interpreted in light of the specification. However, specification states data configuration parameters are stored on servers as data objects that constitute the communication and identification parameters (pg.27, lines 3-5). The specification simply recites configuration parameters and detects communication errors (pg.27, lines 9-13). Examiner does not find the specification reciting the occurrence of communication error can be interpreted as the cause of the communication error or interpreting claimed otherwise.

As discussed above, Britt discloses data includes various configuration parameters (i.e. images, sounds, connection scripts used to establish communication with the server, etc.), which can also referred as information, instructions, or contents that is downloaded and stored in the flash memory (col.7, lines 50-55). Thus, the data that includes configuration parameter relates to communication information, instructions, or content. Hence, Britt reads on the claimed configuration parameter. The term occurrence is defined as something that occurs or the action or instance of occurring. The claimed configuration parameter associated with the occurrence of said communication error can broadly be given as an error condition where an error occurs associated to a configuration parameter or configuration data that has been detected and identified as inconsistent state or error data that has been communicated in the

network (col.8, lines 15-16). Britt discloses the system detects an error condition by verifying which includes a process of identifying if the contents in the flash memory are valid or invalid (col.8, lines 10-11). Based on the broadly claimed occurrence of the communication error and related support in the specification, Britt reads on the claimed invention.

The argument where Britt discloses communication with the network is restored and thereafter the configuration is corrected which the replaced data is not used to restore communication with the network as claimed is traversed. The claimed automatically installing corrected configuration data to restore communication with the network broadly suggest the communication is to be continued or to regain communication once valid or corrected configuration is replaced with the invalid configuration data associated with the communication error. Britt teaches the processing system includes detection means for detecting an interruption in the downloading process (col.3, lines 1-4) and determines whether a download should take place (col.8, lines 12-13). Detecting an interruption and determining a download suggests the communication is stopped or discontinues until it is determined a download is valid where correct information is replaced with the corrupt information (col.8, lines 29-39) associated with the detected error (col.8, lines 10-11 and 15-16). Britt allows errors in the programming or data to be detected and automatically corrected by performing the error download routine with out intervention by the user (col.8, lines 35-39). Thus, Britt reads on the claimed automatically installing the corrected configuration data to restore communications with the network.

All dependent claims are also rejected by virtue of their dependencies.

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100